Cyber Security Workshop

timeless

Can your business afford to avoid this issue any longer?

The Reality in 2025/26: 43% of UK businesses faced a cyber breach or attack in the past year, with around 612,000 businesses affected.
(Source: Cyber Security Breaches Survey 2025 – GOV.UK)

A Serious Data Breach Can Cost You:

- Heavy ICO fines and mandatory reporting
- Forced client notifications with an instant loss of trust
- Severe reputational damage that hits sales
- Weeks of business downtime while systems are offline

timeless

Building Cyber Resilience — Why Time Is Your Most Critical Asset

The Reality of Modern Cyber Risks — A Race Against Time

Cyberattacks are fast, automated, and unforgiving.

Myth-busting:

- **“Cybersecurity is only for big businesses.”**
- **“We are too small to be targeted.”**
- **“IT handles it all.”**

Reality check:

60% of SME breaches start with phishing or weak passwords.
Cost is not just downtime, reputation and trust are at stake.
Recent supply chain breaches (Harrods, Jaguar Land Rover): minutes matter.

timeless

Your Business Growth. Accelerated by Technology

The Building Blocks of Resilience

PROTECTION:
EDR, MFA, backups, email filtering, staff awareness

DETECTION:
Continuous monitoring, instant alerts, vulnerability scans

RESPONSE:
Incident response plan and regular tabletop exercises

RECOVERY:
Tested backups, clear comms, post-mortem reviews

timeless

Your Business Growth. Accelerated by Technology

The Building Blocks of Resilience

	SME A (Minimal Layers)	SME B (MSP-Driven Resilience Plan)
Protection	Basic antivirus, no MFA, staff unaware of phishing	EDR, MFA for all, regular staff training on threats
Detection	No active monitoring, no alert system	24/7 monitoring, real-time alerts, regular vulnerability scans
Response	No clear incident response plan, ad hoc handling	Documented IR plan, practice tabletop exercises with clear roles
Recovery	Unreliable, untested backups, no clear recovery steps	Regularly tested backups, fast recovery protocols, post-incident reviews
Business Impact	Higher risk of breach, slow response, longer downtime, reputational damage	Rapid incident containment, reduced downtime, improved client trust

Time as a Strategic Advantage for Growth

Security speed enables faster innovation, improves delivery and builds trust.

“Cyber resilience as a competitive advantage:”

- **Improved uptime**
- **Faster customer delivery**
- **Protected reputation**

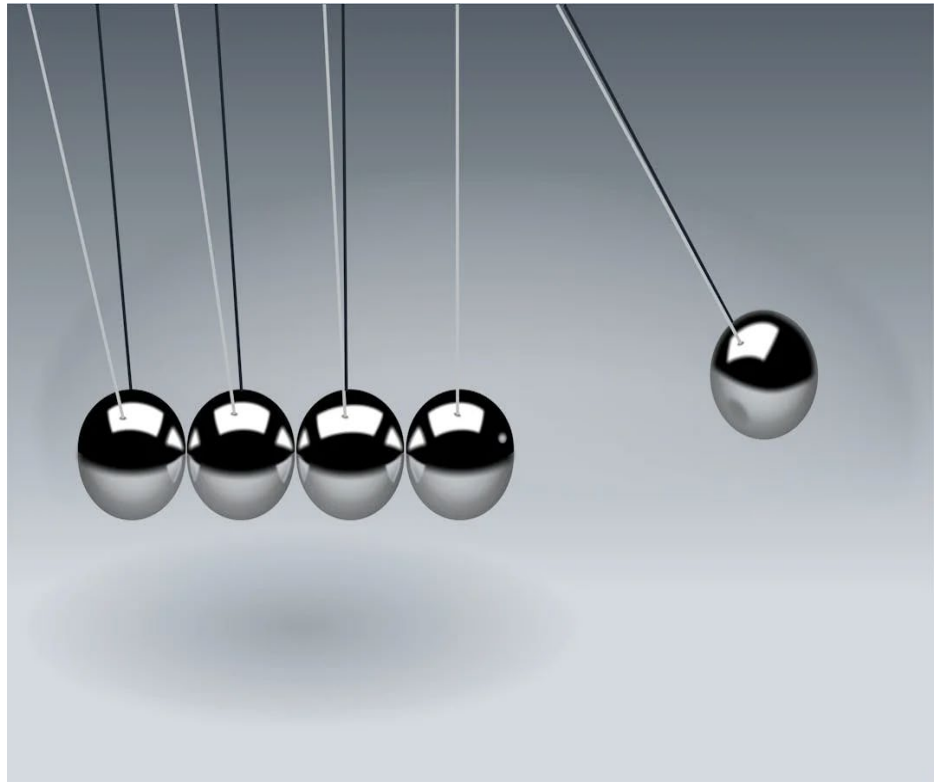
Security is not a cost.. it is an investment.

timeless

Your Business Growth. Accelerated by Technology

Practical SME Steps to Gain Time Advantage

1. Run a phishing drill.
2. Enable MFA for all cloud/user accounts.
3. Audit your backup and test recovery speed.
4. Review supply chain security
   & challenge vendors for their verification.
5. Draft an incident communication plan



timeless

Your Business Growth. Accelerated by Technology

Cultivating a Time-Conscious Cyber Culture

1. **Leadership drives preparation (not panic).**
2. **Reward staff who spot risks early.**
3. **Run quarterly “cyber health checks” or resilience drills, include every department.**

timeless

Your Business Growth. Accelerated by Technology

Every Second Counts

RECAP: Resilience = protection, detection, response, recovery.

CHALLENGE: Are you ready to act when every second matters?

INVITE: Complimentary cyber health scan or resilience tabletop drill with Timeless IMS.

QUOTE: “The future belongs to those who prepare fastest.”

timeless

Your Business Growth. Accelerated by Technology

Key Recent Cybersecurity Insights in the Construction Sector

Manufacturing Remains the #1 Target for Cyberattacks

Automotive Manufacturing Tops Strategic Priorities for Cybersecurity

timeless

Your Business Growth. Accelerated by Technology

Cybersecurity Insights

Microsoft 365 Password Expiration Alert

Subject: Urgent: Your Microsoft 365 password expires in 24 hours

From: Microsoft Account Team <security@microsoft-365-alert.com>

Body preview: Dear User, Your password is set to expire today to maintain security compliance. Failure to update will result in temporary suspension of email, Teams, and OneDrive access. Click here to update now.

timeless

Your Business Growth. Accelerated by Technology

HR Document Signature Required

Subject: Updated Remote Work Policy – Action Required by EOD

From: HR Department <hr@yourcompanyhr.net>

Body preview: Team, Attached is the new remote work policy effective immediately. Please review, sign electronically, and return via the secure link below to confirm receipt. This is mandatory per company compliance.

timeless

Your Business Growth. Accelerated by Technology

Cybersecurity Insights

CEO/Executive Quick Request (BEC style)

Subject: Quick Favor – Need Your Help ASAP

From: Michael Ramlakhan<ceo@timelessims.com>

Body preview: Hi Stuart, I'm in back-to-back meetings and need you to handle a confidential supplier payment urgently. Please process £4,850 to the new account details attached and confirm once done. Keep this between us. Thanks!

timeless

Your Business Growth. Accelerated by Technology

Bank Security Alert / Unusual Activity

Subject: Action Required: Unusual Login Attempt Detected

From: Security Alerts <alerts@chase-secure.com>

Body preview: We blocked a sign-in attempt from an unrecognised device in Twickenham. To secure your account, verify your identity immediately. Click below to review and confirm.

Google Docs / Shared Document Notification

Subject: Michael Ramlakhan shared "Q4 Budget Review" with you

From: Google Drive <no-reply@drive-google.com>

Body preview: Michael has invited you to view and comment on the attached document. Open now to review changes before tomorrow's meeting.

timeless

Your Business Growth. Accelerated by Technology

Invoice / Supplier Payment Update

Subject: Past Due Invoice #INV-478912 – Immediate Payment Required

From: Accounts Payable <billing@timelessims.com>

Body preview: Our records show invoice #478912 is overdue. Updated payment details attached. Please remit via the secure portal to avoid service interruption.

timeless

Your Business Growth. Accelerated by Technology

Account Verification / "Keep Your Account Active"

Subject: Your account requires immediate verification

From: Netflix Support <account@netflix-verify.net>

Body preview: Due to recent suspicious activity, your Netflix account is on hold. Verify your payment method and details within 48 hours to reactivate and avoid cancellation.

Job Offer / Research Assistant Opportunity

Subject: Research Assistant Position – Weekly Compensation Provided

From: Recruitment Team <careers@prestigious-university.org>

Body preview: We are seeking motivated individuals for a remote research role with flexible hours and £750 weekly stipend. Submit your details and availability via the link to apply. Limited spots available.

Package Delivery / Customs Fee

Subject: Your package is awaiting clearance – Action needed

From: DHL Express <notification@dhl-support.net>

Body preview: A shipment to you is held at customs due to unpaid fee of £2.99. Pay now to release your package. Track and pay here.

Cybersecurity Insights

Here are a few realistic smishing (SMS phishing) text message examples.
These are based on prevalent 2025–2026 trends, including fake delivery issues (still dominant due to online shopping), unpaid fees, bank alerts, urgent account verifications, job offers, and emerging personalised or "cute" lures to build rapport.

Smishing often uses short, urgent language, spoofed sender IDs (shown as short codes or company names), malicious shortened links (e.g., bit.ly), or requests to reply/call.

Fake USPS Package Delivery Issue

Sender: USPS

Message: "USPS: Your package is pending delivery due to an unpaid shipping fee of £2.99. Confirm details & pay to avoid return: [shortened link]"

Job Offer / Urgent Hiring
Sender: HR Recruit
Message: "URGENT HIRING: Remote role £700/day. Flexible hours. Submit details & start ASAP: [link]. Limited spots!"

timeless
Your Business Growth. Accelerated by Technology

Service Suspension Threat

Sender: British Gas

Message: "Your electricity account is past due. Pay £49.99 now to avoid shutoff today: [link]. Ref #123456"

Cybersecurity Insights

Tabletop + Mini Incident Response

Scenario: Ransomware hit a small company (encrypted files + ransom note).:

A small company (e.g., 20–50 employees, local accounting firm or retail business) discovers encrypted files across servers and workstations, plus a ransom note (e.g., README.txt demanding Bitcoin payment with a 72-hour deadline, threatening data leak/publication).

I am looking for answers:

- First actions?
- Who to notify?
- Containment steps?
- Evidence to preserve?

timeless

Your Business Growth. Accelerated by Technology

Michael Ramlakhan

Founder & Managing Director of Timeless IMS. Your Managed Security Service Provider (MSSP) for SME Tech-f...

Thank you for listening

timeless

Your Business Growth. Accelerated by Technology